目录

[漏洞描述 1](#_Toc35437156)

[风险等级 1](#_Toc35437157)

[影响范围 1](#_Toc35437158)

[处置建议 1](#_Toc35437159)

[技术分析 1](#_Toc35437160)

## 漏洞描述

近日，知名Java Json组件Fastjson被发现存在远程拒绝服务漏洞，攻击者可以通过提交精心构造的JSON数据解析到特定字符触发OOM故障，从而实现拒绝服务攻击。该漏洞影响最新1.2.60之前所有Fastjson版本。

## 风险等级

高危 （一般事件）

## 影响范围

该漏洞影响Fastjson 1.2.60之前所有版本。

## 处置建议

升级到最新版本1.2.60。

如果遇到不兼容问题，可以使用如下兼容版本：

1.1.15~1.1.31→1.1.31.sec07

1.1.32~1.1.33→1.1.33.sec06

1.1.34→1.1.34.sec06

1.1.35~1.1.46 →1.1.46.sec06

1.2.3~1.2.7→1.2.7.sec06或1.2.8.sec04

1.2.8→1.2.8.sec06

1.2.9~1.2.29→1.2.29.sec06

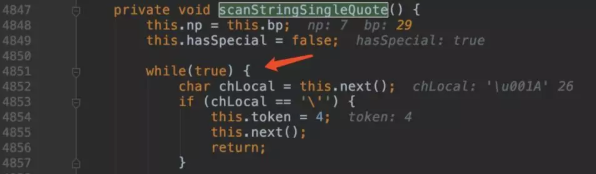
## 技术分析

造成此漏洞的原因有二：

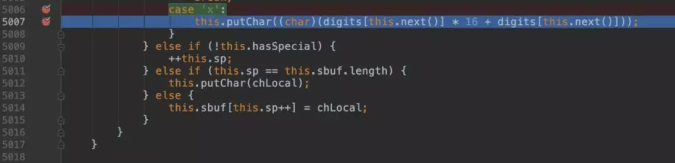
1.Fastjson在处理\x转义字符（十六进制数）时没有对转义字符后的字符进行有效性校验

2.错误的EOF判断逻辑导致字符串读取到结尾时没有跳出循环

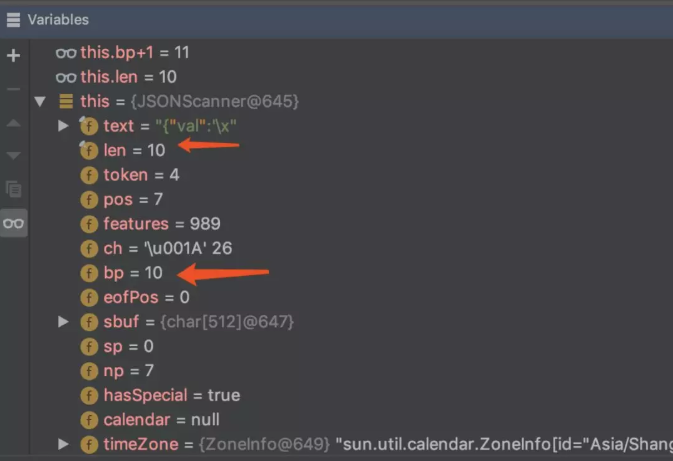
根据漏洞成因和PoC，可以在com/alibaba/fastjson/parser/JSONLexerBase.class的5007行scanStringSingleQuote()方法中的处理转义字符x的分支下断点去跟踪，需要注意的是其判断分支在一个循环中：



断点命中后，我们发现其试图读取此字符串位置的下一个字符和下下个字符去做一个16进制转10进制的转换：



此时我们看下this变量：

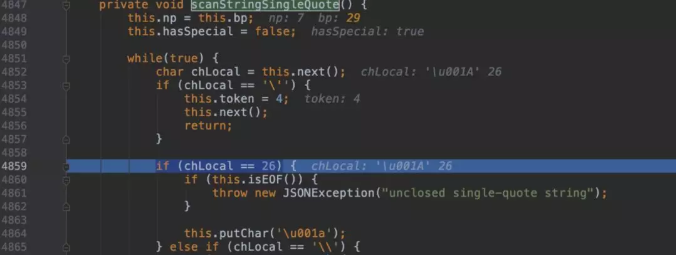


注意此时bp指针为10，和len相等。继续跟踪到com/alibaba/fastjson/parser/JSONScanner.class的44行this.next()方法：



我们发现其读取下一个字符的逻辑是先将bp指针+1然后读取字符。但根据PoC，我们得知下一个字符已经不存在，因此按照其逻辑返回ascii码为26(0x1A)的控制字符。

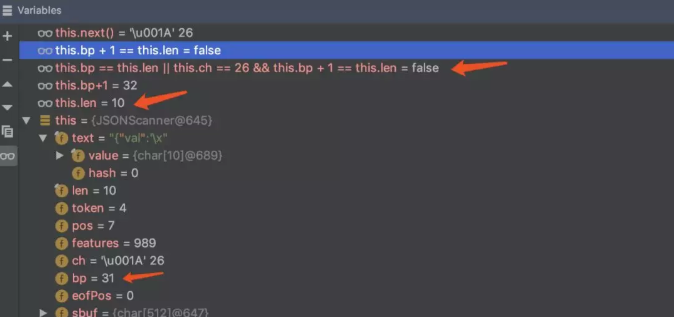
一个循环执行完成进入下一个循环后，再次执行this.next()方法得到控制字符26(0x1A)，进入了if(chLocal == 26)分支：



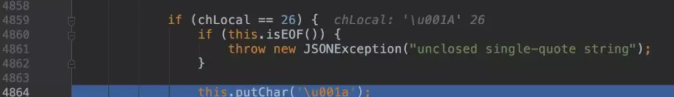
继续跟入this.isEOF()判断：



由于此时bp指针大于字符串长度，错误的EOF判断逻辑导致其返回永远为false：



于是程序继续运行下一次循环：



如此循环往复，直至堆溢出，导致OutOfMemoryError错误，程序崩溃。